9110-04

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2014-0071]

Privacy Act of 1974; Department of Homeland Security /United States Coast Guard – 017 Federal Medical Care Recovery Act System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue a current Department of Homeland Security system of records titled, "Department of Homeland Security/United States Coast Guard Federal Medical Care Recovery Act System of Records." This system of records allows the Department of Homeland Security/United States Coast Guard to collect and maintain Federal Medical Care Recovery Act claims (FMCRA). As a result of the biennial review of this system, the system manager and address category has been updated. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This updated system will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2014-0071 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

DOCKET: For access to the docket to read background documents or comments received, please visit http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Marilyn Scott-Perez (202) 475-3515, Privacy Officer, Commandant (CG-61), United States Coast Guard, Mail Stop 7710, Washington, D.C. 20593. For privacy questions, please contact: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) United States Coast Guard (USCG) proposes to update and reissue a current DHS system of records titled, "DHS/United States Coast Guard-017

Federal Medical Care Recovery Act System of Records. The collection and maintenance of this information will assist DHS/USCG in meeting its statutory obligation to address FMCRA claims. As a result of a biennial review of the system, the system manager and address category has been updated to reflect the new mail stop.

Consistent with DHS's information-sharing mission, information stored in the DHS/USCG-017 Federal Medical Care Recovery Act System of Records may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice. This updated system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records

maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/USCG-017 Federal Medical Care Recovery Act System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records

Department of Homeland Security (DHS)/USCG-017

System name:

DHS/USCG-017 Federal Medical Care Recovery Act.

Security classification:

Unclassified

System location:

Records are maintained at the United States Coast Guard Headquarters in Washington, D.C. and field offices and at USCG health care facilities where the USCG military personnel or eligible dependent receives treatment.

Categories of individuals covered by the system:

Categories of individuals covered by this system include active duty, reserve, and retired active duty, retired reserve, and their eligible dependents. Also included are insurance company employees, related legal staff, the alleged tortfeasor. Finally, individuals such as Search and Rescue victims, employees, volunteers, or others who are provided emergency care by the USCG.

Categories of records in the system:

Categories of records in this system include:

- Military personnel's name;
- Eligible dependent's name;
- Social Security number;
- Gender;
- Date of birth;
- Case number;
- Insurance company's name and representative's name;
- Legal firm's name and legal representative's name;
- Addresses;
- Telephone numbers;
- Correspondence, memoranda, and related documents concerning potential and actual FMCRA claims;
- Police reports;
- Witness statements;
- Court documentation;
- Basic contact information for insurance companies, legal staff, and tortfeasor;
- Copies of medical and dental treatment provided to the individual subject of the claim;

- Copies of medical bills associated with civilian care provided at government expense; and
- Automated data processing (ADP) records containing identifying data on individuals, unit of assignment and address, home address, the amount of the claim, the amount paid to the government on the claim, dates of correspondence sent, due dates of reply, claim number, date claim opened, and date claim closed.

Authority for maintenance of the system:

Departmental Regulations, 5 U.S.C. 301; the Federal Records Act, 44 U.S.C. § 3101; 14 U.S.C. 632.; 10 U.S.C. 1095, Uniformed Services Medical and Dental Care; 42 U.S.C. 2651 et seq., Federal Medical Care Recovery Act. 3 CFR 25.131, 133.

Purpose(s):

The purpose of this system is to collect and maintain FMCRA claims for the United States Coast Guard.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Note: For records of identity, diagnosis, prognosis, or treatment of any client/patient, irrespective of whether or when he/she ceases to be a client/patient, maintained in connection with the performance of any alcohol or drug abuse prevention and treatment function conducted, requested, or directly or indirectly assisted by any department or agency of the United States, shall, except as provided therein, be confidential and be disclosed only for the purposes and under circumstances expressly authorized in 42 U.S.C. 290dd-2. The results of a drug test of civilian employees may be

disclosed only as expressly authorized under 5 U.S.C. 7301. These statutes limit disclosures otherwise permitted by the Privacy Act of 1974 to the extent that disclosure is more limited. Thus, the Routine Uses set forth below do not apply to this information. However, access to the record by the individual to whom the record pertains is governed by the Privacy Act.

A. To medical personnel to the extent necessary to meet a bona fide medical emergency;

B. To qualified personnel for the purpose of conducting scientific research, management audits, financial audits, or program evaluation, provided that employees are individually identified;

C. To the employee's medical review official;

D. To the administrator of any Employee Assistance Program in which the employee is receiving counseling or treatment or is otherwise participating;

E. To any supervisory or management official within the employee's agency having authority to take adverse personnel action against such employee; or

F. Pursuant to the order of a court of competent jurisdiction when required by the United States Government to defend against any challenge against any adverse personnel action. See 42 U.S.C. 290dd, 290ee, and Public Law 100-71, Section 503(e).

Note: For all other records besides those noted above, this system of records contains individually identifiable health information. The Health Insurance Portability and Accountability Act of 1996 applies to most of such health information. Department of

Defense 6025.18-R may place additional procedural requirements on the uses and disclosures of such information beyond those found in the Privacy Act of 1974 or mentioned in this system of records notice. Therefore, routine uses outlined below may not apply to such health information.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records of information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice including Offices of the United States Attorneys or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee of DHS in his/her official capacity;

3. Any employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration (GSA) pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity); and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To attorneys and insurance companies involved in settling and litigating claims pursuant to Health Information Portability and Accountability Act.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

USCG stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, or digital media.

Retrievability:

USCG may retrieve records by name, Social Security number, case number, or address of military personnel or eligible dependent. USCG can also retrieve records by attorney's or other parties' names.

Safeguards:

USCG safeguards records in this system in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. USCG imposes strict controls to minimize the risk of compromising the information. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

USCG retains records at USCG Headquarters for 2 years; transfers the records to a Federal Records Center for an additional 4 years, for a total of 6 years, and destroys the records thereafter. (AUTH: GRS 1, Item 19.)

System Manager and address:

Commandant (CG-1), United States Coast Guard, Mail Stop 7907, Washington, D.C. 20593-0001.

Notification procedure:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Commandant (CG-611), United States Coast Guard, Mail Stop 7710, Washington, D.C. 20593. If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See "Notification procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

USCG obtains records from the individual, or if a minor, the parent or guardian, and witnesses; Medical facilities (USCG, Department of Defense, Uniformed Services Treatment Facility, or Civilian Facility) where beneficiaries are treated; injury investigations, attorneys, and insurance companies involved in the claim.

Exemptions claimed for the system:

None.

Dated: November 18, 2014.

Karen L. Neuman,

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2014-29349 Filed 12/15/2014 at 8:45 am; Publication Date: 12/16/2014]